Amendments to the Claims

1. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message M between a sender and a recipient with participation of an authorizer ~~as specified by operations (a) through (f) defined below~~, wherein the digital message is encrypted by the sender and decrypted by the recipient, the method comprising encrypting, by at least one machine in a set of one or more machines, the digital message M using at least a recipient public key and a recipient encryption key to create an encrypted digital message for decryption with a recipient private key and a recipient decryption key, wherein:

~~one or more of operations (R), (Au), (S), wherein:~~

~~the operation (R) comprises the operations (a), (f);~~

~~the operation (Au) comprises the operations (c), (d);~~

~~the operation (S) comprises the operation (e);~~

~~wherein the operations (a) through (f) are as follows:~~

~~(a) generating~~ the recipient public key and the recipient private key form a ~~recipient~~ public key/ ~~recipient~~ private key pair, wherein the recipient private key is a secret of the recipient;

~~(b) generating a recipient encryption key;~~

~~(c) selecting a key generation secret that is a secret of the authorizer;~~

~~(d) generating a~~ the recipient decryption key is generated using at least [[the]] a key generation secret of the authorizer and the recipient encryption key, wherein a key formed from the recipient ~~decryption~~ encryption key and a key formed from the recipient ~~encryption~~ decryption key are a public key/ private key pair. [[;]]

~~(e) enerypting the digital message using at least the recipient public key and the recipient encryption key to create an encrypted digital message; and~~

~~(f) decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key.~~

2. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

3. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

4. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising the recipient public key.

5. (Original) The method of claim 1, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

6. (Original) The method of claim 1, wherein the recipient decryption key is generated by the authorizer according to a schedule known to the sender.

7. (Original) The method of claim 6, wherein the recipient encryption key is generated using at least information comprising the schedule.

8. (currently amended) The method of claim 1, wherein the recipient private key [[/]] and the recipient public key ~~pair is~~ are generated using at least one system parameter issued by the authorizer.

9. (currently amended) The method of claim 1, wherein ~~generating the recipient decryption key comprises~~ the recipient decryption key is generated by the authorizer to have a value $S = s_E P_B$, wherein:

s_E is the key generation secret of the authorizer; and

P_B is the recipient encryption key and is equal to $H_1(\text{Inf}_B)$, wherein Inf_B is an element of ~~generating~~ a first cyclic group $\mathbb{G}_1$ of elements, wherein P_B is an element of ~~and~~ a second cyclic group $\mathbb{G}_2$ of elements, and H_1 is a predefined function ("first function H_1"), wherein the first and second cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and the function H_1 are system parameters made available to the sender, and also available to the sender are system parameters comprising:

~~selecting a function $\hat{e}$ capable of generating an element of the second cyclic group $\mathbb{G}_2$ from two elements of the first cyclic group $\mathbb{G}_1$;~~

~~selecting~~ a generator P of the first cyclic group $\mathbb{G}_1$;

~~selecting a random key generation secret s_C associated with and known to authorizer;~~

~~generating~~ a key generation parameter $Q = s_C P$;

~~selecting a first function H_1 capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a first string of binary digits;~~

~~selecting~~ a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$. [[;]]

~~generating an element $P_B = H_1(\text{Inf}_B)$, wherein Inf_B comprises a string of binary digits; and~~

~~generating a secret element $S = s_e P_B$ associated with the recipient, wherein the secret element is the recipient decryption key.~~

10. (Original) The method of claim 9, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

11. (Original) The method of claim 9, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

12. (Original) The method of claim 9 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

13. (currently amended) The method of claim 9 wherein the system parameters available to the sender further comprise [[the]] a function $\hat{e}$ which is a bilinear, non-degenerate, and efficiently computable pairing which maps $\mathbb{G}_1 \text{ X } \mathbb{G}_1$ into $\mathbb{G}_2$.

14. (currently amended) The method of claim [[9]] 11 wherein:

s_C is an element of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ [[;]] .

~~Q is an element of the second cyclic group $\mathbb{G}_2$;~~

~~element P_B is an element of the first cyclic group $\mathbb{G}_1$; and~~

~~the secret element S is an element of the first cyclic group $\mathbb{G}_1$.~~

15. (currently amended) The method of claim 9, wherein encrypting the digital message M comprises:

generating [[the]] an element $P'_B = H_1(ID_{rec})$, wherein ID_{rec} comprises the identity of the recipient and wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

selecting a random key generation secret *r;* and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, where PK_B is the recipient public key and wherein ê is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 X \mathbb{G}_1$ into $\mathbb{G}_2$.

16. (Original) The method of claim 1, wherein the recipient encryption key is generated from a document and the recipient decryption key is the authorizer's signature on the document.

17. (currently amended) The method of claim [[9]] 11, wherein encrypting the digital message M comprises:

generating [[the]] an element $P'_B = H_1(ID_{rec})$ wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

choosing a random parameter $\sigma \in \{0,1\}^n$;

set a random key generation secret $r = H_3(\sigma, M)$; and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r), E_{H_4(\sigma)}(M)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, wherein PK_B is the recipient public key, wherein H_3 is a function capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from two strings of binary digits, H_4 is a function capable of generating one binary string from another binary string, E is a symmetric encryption scheme, ê is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 X \mathbb{G}_1$ into $\mathbb{G}_2$, and $H_4(\sigma)$ is the key used with E.

18. (currently amended) A method for operating a public-key encryption scheme which provides for sending a digital message between a sender and a recipient with

participation of a plurality of authorizers ~~as specified by operations (a) through (g) defined below~~ , the plurality of authorizers including a root authorizer and *n* lower-level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, the method comprising encrypting, by at least one machine in a set of one or more machines, the digital message using a recipient public key and a recipient encryption key to create an encrypted digital message for decryption with a recipient private key and a recipient decryption key, wherein:

a key formed from the recipient encryption key and a key formed from the recipient decryption key are a public key/ private key pair;

~~one or more of operations (R), (RAu), (Au), (S), wherein:~~

~~the operation (R) comprises the operations (a), (g);~~

~~the operation (RAu) comprises the operations (e), (d);~~

~~the operation (Au) comprises the operation (e);~~

~~the operation (S) comprises the operation (f);~~

~~wherein the operations (a) through (g) are as follows:~~

~~(a) generating a~~ the recipient public key [[/]] and the recipient private key form a public key/private key pair ~~for the recipient~~ , wherein the recipient private key is a secret of the recipient;

~~(b) generating a~~ the recipient encryption key is generated using identity information of at least one of the recipient's ancestors;

~~(c) selecting a root key generation secret that is a secret of the root authorizer;~~

~~(d) generating a root key generation parameter based on the root key generation secret;~~

~~(e) generating a~~ the recipient decryption key is generated such that the recipient decryption key is related to the recipient encryption key, [[the]] a root key generation secret and [[the]] an associated root key generation parameter, wherein the root key generation parameter is generated based on the root key generation secret, and the root key generation secret is a secret of the root authorizer. [[;]]

~~(f) encrypting the digital message using the recipient public key and a recipient encryption key to create an encrypted digital message, wherein a key formed from the~~

~~recipient decryption key and a key formed from the recipient encryption key are a public key/ private key pair; and~~

~~(g) decrypting the encrypted digital message to recover the digital message using at least the recipient private key and the recipient decryption key.~~

19. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

20. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

21. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising the recipient public key.

22. (Original) The method of claim 18, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

23. (Original) The method of claim 18, wherein the recipient decryption key is generated according to a schedule known to the sender.

24. (currently amended) The method of claim 18, wherein the recipient private key [[/]] and the recipient public key ~~pair is~~ are generated using system parameters issued by one or more of the authorizers.

25. (Original) The method of claim 18, wherein the recipient decryption key is related to the root key generation secret and the associated root key generation parameter.

26. (currently amended) The method of claim 18, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein l of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is

the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, and wherein ~~the the public-key encryption scheme further comprising~~ :

~~selecting~~ a lower-level key generation secret is selected for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

~~generating~~ a sender decryption key is generated such that the sender decryption key is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least the sender decryption key and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers above the lowest common ancestor authorizer$_l$; and

wherein the encrypted digital message is ~~decrypted~~ decryptable using at least the recipient decryption key and one or more of the lower-level key generation parameters associated with the $(n - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers that above the lowest common ancestor authorizer$_l$.

27-116. (cancelled)

117. (currently amended) The method of claim 1 wherein the method further comprises ~~the operation (R) performed by~~ the recipient performing, by at least one machine in the set of the one or more machines, operations of:

generating the recipient public key and the recipient private key;

decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key.

118. (currently amended) The method of claim 1 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating the recipient decryption key and sending the recipient decryption key to the recipient.

119. (canceled)

120. (currently amended) The method of claim [[1]] 118 wherein the method further comprises ~~the operation (R) performed by~~ the recipient ~~and the operation (Au) performed by the authorizer~~ performing, by at least one machine in the set of the one or more machines, operations of:

generating the recipient public key and the recipient private key;

decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key.

121-123. (canceled)

124. (currently amended) The method of claim 1 ~~wherein the operation (b) is performed~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key by the authorizer and/or the recipient and/or the sender.

125. (currently amended) The method of claim 2 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

126. (currently amended) The method of claim 3 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~126~~ 127. (currently amended) The method of claim 4 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~127~~ 128. (currently amended) The method of claim 5 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~127~~ 129. (currently amended) The method of claim 6 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~129~~ 130. (currently amended) The method of claim 7 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~130~~ 131. (currently amended) The method of claim 9 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~131~~ 132. (currently amended) The method of claim 10 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~132~~ 133. (currently amended) The method of claim 11 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~133~~ 134. (currently amended) The method of claim 12 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~134~~ 135. (currently amended) The method of claim 13 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~135~~ 136. (currently amended) The method of claim 14 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~136~~ 137. (previously presented) The method of claim 15 wherein the method comprises the operation (S) performed by the sender.

~~137~~ 138. (currently amended) The method of claim 16 wherein the method further comprises ~~the operation (Au) performed by~~ the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

~~138~~ 139. (currently amended) The method of claim 16 wherein the method further comprises ~~the operation (R) performed by~~ the recipient performing, by at least one machine in the set of the one or more machines, operations of:

generating the recipient public key and the recipient private key;

decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key.

~~139~~ 140. (canceled)

~~140~~ 141. (currently amended) The method of claim 18 wherein the method further comprises ~~the operation (R) performed by~~ the recipient performing, by at least one machine in the set of the one or more machines, operations of.

generating the recipient public key and the recipient private key; and

decrypting the encrypted digital message to recover the digital message using at least the recipient private key and the recipient decryption key.

~~141~~ 142. (currently amended) The method of claim 18 wherein the method further comprises ~~the operation (RAu) performed by~~ the root authorizer performing, by at least one machine in the set of the one or more machines, operations of:

selecting the root key generation secret that is a secret of the root authorizer; and

generating the root key generation parameter based on the root key generation secret.

~~142~~ 143. (currently amended) The method of claim 18 wherein the method further comprises ~~the operation (Au) performed~~ generating, by at least one machine in the set of the one or more machines, the recipient decryption key by one of the authorizers.

~~143~~ 144. (canceled)

~~144~~ 145. (currently amended) The method of claim [[18]] 142 wherein ~~the method comprises the operation (R) performed by the recipient and the operation (Au)~~

~~performed by one of the authorizers~~ further comprising the recipient performing, by at least one machine in the set of the one or more machines, operations of.

generating the recipient public key and the recipient private key; and

decrypting the encrypted digital message to recover the digital message using at least the recipient private key and the recipient decryption key.

~~145~~ 146. (canceled)

~~146~~ 147. (canceled)

~~147~~ 148. (canceled)

~~148~~ 149. (currently amended) The method of claim 18 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~149~~ 150. (currently amended) The method of claim 19 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~150~~ 151. (currently amended) The method of claim 20 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~151~~ 152. (currently amended) The method of claim 21 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~152~~ 153. (currently amended) The method of claim 22 ~~wherein the method comprises the operation (b)~~ further comprising generating, by at least one machine in the set of the one or more machines, the recipient encryption key.

~~153~~ 154. (currently amended) The method of claim 23 wherein the method further comprises ~~the operation (Au) performed~~ generating, by at least one machine in the set of the one or more machines, the recipient decryption key by one of the authorizers.

~~154~~ 155. (currently amended) The method of claim 25 wherein the method further comprises ~~the operation (Au) performed~~ generating, by at least one machine in the set of the one or more machines, the recipient decryption key by one of the authorizers.

156. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 1.

157. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 5.

158. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 9.

159. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 10.

160. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 11.

161. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 13.

162. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 15.

163. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 16.

164. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 17.

165. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 18.

166. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 20.

167. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 22.

168. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 23.

169. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 26.

170. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 117.

171. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 118.

172. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 119.

173. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 123.

174. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 127.

175. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 130.

176. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 136.

177. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 140.

178. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 141.

179. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 142.

180. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 143.

181. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 147.

182. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 150.

183. (currently amended) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 152.

184. (new) A method for operating a public-key encryption scheme which provides for sending a digital message M between a sender and a recipient with participation of an authorizer, wherein the digital message M is encrypted by the sender using at least a recipient public key and a recipient encryption key to create an encrypted digital message and is decrypted by the recipient, the method comprising decrypting, by at least one machine in a set of one or more machines, the encrypted digital message using at least a recipient private key and a recipient decryption key, wherein:

the recipient public key and the recipient private key form a public key/ private key pair, wherein the recipient private key is a secret of the recipient;

the recipient decryption key is generated using at least a key generation secret of the authorizer and the recipient encryption key, wherein a key formed from the recipient encryption key and a key formed from the recipient decryption key are a public key/ private key pair.

185. (new) The method of claim 184, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

186. (new) The method of claim 184, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

187. (new) The method of claim 184, wherein the recipient encryption key is generated from information comprising the recipient public key.

188. (new) The method of claim 184, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key

189. (new) The method of claim 184, wherein the recipient decryption key is generated by the authorizer according to a schedule known to the sender.

190. (new) The method of claim 189, wherein the recipient encryption key is generated using at least information comprising the schedule.

191. (new) The method of claim 184, wherein the recipient private key and the recipient public key are generated using at least one system parameter issued by the authorizer.

192. (new) The method of claim 184, wherein the recipient decryption key is generated by the authorizer to have a value $S = s_c P_B$, wherein:

s_c is the key generation secret of the authorizer; and

P_B is the recipient encryption key and is equal to $H_1(\text{Inf}_B)$, wherein Inf_B is an element of ~~generating~~ a first cyclic group $\mathbb{G}_1$ of elements, wherein P_B is an element of ~~and~~ a second cyclic group $\mathbb{G}_2$ of elements, and H_1 is a predefined function ("first function H_1"), wherein the first and second cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and the function H_1 are system parameters made available to the sender, and also available to the sender are system parameters comprising:

a generator P of the first cyclic group $\mathbb{G}_1$;

a key generation parameter $Q = s_C P$;

a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$.

193. (new) The method of claim 192, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

194. (new) The method of claim 192, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

195. (new) The method of claim 192 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

196. (new) The method of claim 192 wherein the system parameters available to the sender further comprise a function $\hat{e}$ which is a bilinear, non-degenerate, and efficiently computable pairing which maps $\mathbb{G}_1 \text{ X } \mathbb{G}_1$ into $\mathbb{G}_2$.

197. (new) The method of claim 194 wherein:

s_C is an element of the cyclic group $\mathbb{Z} / q\mathbb{Z}$.

198. (new) The method of claim 192, wherein encrypting the digital message M comprises:

generating an element $P'_B = H_1(\text{ID}_{\text{rec}})$, wherein ID_{rec} comprises the identity of the recipient and wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

selecting a random key generation secret r; and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, where PK_B is the recipient public key and wherein ê is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$.

199. (new) The method of claim 184, wherein the recipient encryption key is generated from a document and the recipient decryption key is the authorizer's signature on the document.

200. (new) The method of claim 194, wherein encrypting the digital message M comprises:

generating an element $P'_B = H_1(ID_{rec})$ wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits;

choosing a random parameter $\sigma \in \{0,1\}^n$;

set a random key generation secret $r = H_3(\sigma, M)$; and

encrypting the digital message M to form a ciphertext C, wherein C is set to be:

$C = [rP, M \oplus H_2(g^r), E_{H_4(\sigma)}(M)]$, where $g = \hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, wherein PK_B is the recipient public key, wherein H_3 is a function capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from two strings of binary digits, H_4 is a function capable of generating one binary string from another binary string, E is a symmetric encryption scheme, ê is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 \times \mathbb{G}_1$ into $\mathbb{G}_2$, and $H_4(\sigma)$ is the key used with E.

201. (new) The method of claim 184 further comprising the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient.

202. (new) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 184.

203. (new) A method for operating a public-key encryption scheme which provides for sending a digital message M between a sender and a recipient with participation of an authorizer, wherein the digital message is encrypted by the sender using at least a recipient public key and a recipient encryption key, wherein the recipient public key and a recipient private key form a recipient public key/ recipient private key pair, wherein the recipient private key is a secret of the recipient, and the digital message is decrypted by the recipient using at least the recipient private key and a recipient decryption key, the method comprising the authorizer performing, by at least one machine in a set of one or more machines, operations of:

selecting a key generation secret that is a secret of the authorizer;

generating a recipient decryption key using at least the key generation secret of the authorizer and the recipient encryption key, wherein a key formed from the recipient encryption key and a key formed from the recipient decryption key are a public key/ private key pair;

sending the recipient decryption key to the recipient.

204. (new) The method of claim 203, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

205. (new) The method of claim 203, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

206. (new) The method of claim 203, wherein the recipient encryption key is generated from information comprising the recipient public key.

207. (new) The method of claim 203, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

208. (new) The method of claim 203, wherein the recipient decryption key is generated by the authorizer according to a schedule known to the sender.

209. (new) The method of claim 208, wherein the recipient encryption key is generated using at least information comprising the schedule.

210. (new) The method of claim 203, wherein the recipient decryption key is generated by the authorizer to have a value $S = s_c P_B$, wherein:

s_c is the key generation secret of the authorizer; and

P_B is the recipient encryption key and is equal to $H_1(\text{Inf}_B)$, wherein Inf_B is an element of a first cyclic group $\mathbb{G}_1$ of elements, wherein P_B is an element of a second cyclic group $\mathbb{G}_2$ of elements, and H_1 is a predefined function ("first function H_1"), wherein the first and second cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and the function H_1 are system parameters made available to the sender, and also available to the sender are system parameters comprising:

a generator P of the first cyclic group $\mathbb{G}_1$;

a key generation parameter $Q = s_C P$;

a second function H_2 capable of generating a second string of binary digits from an element of the second cyclic group $\mathbb{G}_2$.

211. (Original) The method of claim 210, wherein Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

212. (new) The method of claim 210, wherein both the first group $\mathbb{G}_1$ and the second group $\mathbb{G}_2$ are of the same prime order q.

213. (new) The method of claim 210 wherein the first cyclic group $\mathbb{G}_1$ is an additive group of points on a supersingular elliptic curve or abelian variety, and the second cyclic group $\mathbb{G}_2$ is a multiplicative subgroup of a finite field.

214. (new) The method of claim 210 wherein the system parameters available to the sender further comprise a function $\hat{e}$ which is a bilinear, non-degenerate, and efficiently computable pairing which maps $\mathbb{G}_1 \text{ X } \mathbb{G}_1$ into $\mathbb{G}_2$.

215. (new) The method of claim 212 wherein:

s_C is an element of the cyclic group Z/qZ.

216. (new) The method of claim 203, wherein the recipient encryption key is generated from a document and the recipient decryption key is the authorizer's signature on the document.

217. (new) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 203.

218. (new) A method for operating a public-key encryption scheme which provides for sending a digital message between a sender and a recipient with participation of a plurality of authorizers, the plurality of authorizers including a root authorizer and n lower-level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, wherein the digital message is encrypted by the sender using a recipient public key and a recipient encryption key to create an encrypted digital message for decryption by the recipient using a recipient private key and a recipient decryption key,

the method comprising performing, by at least one machine in a set of one or more machines, operations of:

generating the recipient public key and the recipient private key which are a public key/private key pair, wherein the recipient private key is a secret of the recipient;

obtaining an encrypted digital message formed by encryption of the digital message with the recipient public key and the recipient encryption key, wherein a key formed from the recipient encryption key and a key formed from the recipient decryption key are a public key/ private key pair; and

decrypting the encrypted digital message to recover the digital message using at least the recipient private key and the recipient decryption key;

wherein the recipient encryption key is generated using identity information of at least one of the recipient's ancestors;

wherein the recipient decryption key is generated such that the recipient decryption key is related to the recipient encryption key, a root key generation secret and an associated root key generation parameter, wherein the root key generation parameter is generated based on the root key generation secret, and the root key generation secret is a secret of the root authorizer.

219. (new) The method of claim 218, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

220. (new) The method of claim 218, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

221. (new) The method of claim 218, wherein the recipient encryption key is generated from information comprising the recipient public key.

222. (new) The method of claim 218, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

223. (new) The method of claim 218, wherein the recipient decryption key is generated according to a schedule known to the sender.

224. (new) The method of claim 218, wherein the recipient private key and the recipient public key are generated using system parameters issued by one or more of the authorizers.

225. (new) The method of claim 218, wherein the recipient decryption key is related to the root key generation secret and the associated root key generation parameter.

226. (new) The method of claim 218, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein l of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, and wherein:

a lower-level key generation secret is selected for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

a sender decryption key is generated such that the sender decryption key is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least the sender decryption key and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers above the lowest common ancestor authorizer$_l$; and

wherein the encrypted digital message is decryptable using at least the recipient decryption key and one or more of the lower-level key generation parameters associated with the $(n - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers that above the lowest common ancestor authorizer$_l$.

227. (new) The method of claim 218 further comprising generating, by at least one machine in the set of the one or more machines, the recipient decryption key by one of the authorizers.

228. (new) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 218.

229. (new) A method for operating a public-key encryption scheme which provides for sending a digital message between a sender and a recipient with participation of a plurality of authorizers, the plurality of authorizers including a root authorizer and n lower-

level authorizers in a hierarchy between the root authorizer and the recipient, wherein $n \geq 1$, wherein the digital message is encrypted by the sender using a recipient public key and a recipient encryption key to create an encrypted digital message for decryption by the recipient using a recipient private key and a recipient decryption key,

the method comprising generating, by at least one machine in a set of one or more machines, the recipient decryption key such that the recipient decryption key is related to the recipient encryption key, a root key generation secret and an associated root key generation parameter, wherein the root key generation parameter is generated based on the root key generation secret, and the root key generation secret is a secret of the root authorizer;

wherein the recipient encryption key is generated using identity information of at least one of the recipient's ancestors;

wherein a key formed from the recipient encryption key and a key formed from the recipient decryption key are a public key/ private key pair;

wherein the recipient public key and the recipient private key are a public key/private key pair, wherein the recipient private key is a secret of the recipient.

230. (new) The method of claim 229, wherein the recipient encryption key is generated from information comprising the identity of the recipient.

231. (new) The method of claim 229, wherein the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key.

232. (new) The method of claim 229, wherein the recipient encryption key is generated from information comprising the recipient public key.

233. (new) The method of claim 229, wherein the recipient encryption key is generated from information comprising the identity of the recipient, the recipient public key, and a parameter defining a validity period for the recipient decryption key.

234. (new) The method of claim 229, wherein the recipient decryption key is generated according to a schedule known to the sender.

235. (new) The method of claim 229, wherein the recipient private key and the recipient public key are generated using system parameters issued by one or more of the authorizers.

236. (new) The method of claim 229, wherein the recipient decryption key is related to the root key generation secret and the associated root key generation parameter.

237. (new) The method of claim 229, wherein the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein $m \geq 1$, and wherein l of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein $l \geq 1$, and wherein:

a lower-level key generation secret is selected for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and

a sender decryption key is generated such that the sender decryption key is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender;

wherein the message is encrypted using at least the sender decryption key and one or more of the lower-level key generation parameters associated with the $(m - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-level key generation parameters that are associated with the $(l - 1)$ authorizers above the lowest common ancestor authorizer$_l$; and

wherein the encrypted digital message is decryptable using at least the recipient decryption key and one or more of the lower-level key generation parameters associated with the $(n - l + 1)$ authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer$_l$, but not using any of the lower-

level key generation parameters that are associated with the (l - 1) authorizers that above the lowest common ancestor authorizer$_l$.

238. (new) The method of claim 229 further comprising generating, by at least one machine in the set of the one or more machines, the recipient decryption key by one of the authorizers.

239. (new) A computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 229.